УДК 004.415.25

КИБЕРБЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ

Евсигнеева А.Д., Матрунчик Ю. Н.
Белорусский национальный технический университет, г.Минск

На конференции womeninITSummit 2019 было достаточно много материала, посвященного кибербезопасности, так как на сегодняшний день эта тема обретает все большую и большую актуальность. Люди все больше стали заинтересованы в том, чтобы сохранить свою приватность в эру социальных сетей и повышенной компьютеризации. Все чаще и чаще происходят случаи атак и взломов чужих аккаунтов. Не так давно, например, было раскрыто очень много данных о разных людях и их аккаунтах на Facebookв силу бреши в безопасности данных этого сервиса.

На конференции было очень много представителей фирм, занимающихся непосредственно обеспечением кибербезопасности, таких как PaloAltoNetworks, CQUREInc., и отдельные представители отдела технической безопасности различных банков и организации.

Ежедневно происходит огромное количество атак на различные компании, а также появляются новые виды угроз. Для того, чтобы обезопасить себя, фирмы должны проводить для своих сотрудников, особенно тех, у которых есть доступ к засекреченным данным, различные семинары и тренинги, чтобы объяснить и показать насколько важно соблюдать меры осторожности в вопросах доступа к файлам и данным организации.

Одной из важных и полезных лекций на данной конференции была лекция под названием «ThinkandActLikeaHackertoProtectYourCompany’sAssets» (Думай и действуй как хакер для того, чтобы защитить активы свое компании) от представительницы фирмы CQUREInc. Международным экспертом в области кибербезопасности Полы Янушкевич.

Было представлено семь наиболее частых ошибок, совершаемых работниками различных фирм, которые могут привести к потере важнейших данных компании.

1. Не стоит использовать простые пароли

Очень часто в современном офисе у не особенно сведущего работника на рабочем столе можно увидеть большое количество стикеров с паролями от различных рабочих ресурсов. И часто эти пароли достаточно простые, вроде «Пароль», «qwerty» или «123». И если у данного сотрудника есть доступ к файлам, которые не должны попасть в руки других людей, то получить доступ к этим файлам из вне будет достаточно просто даже методом обыкновенного подбора.

Чтобы избежать такой ошибки, следует объяснить персоналу, насколько важно создавать пароль таким, чтобы его не было легко взломать. И не стоит вешать стикеры с паролем на видном месте.

2. Осторожность во время того, когда оставляешь свое рабочее место

В настоящее время очень много людей, оставляя свое рабочее место во время перерыва не блокируют доступ к компьютеру, и любой желающий проходящий мимо человек может сесть за этот компьютер и получить доступ ко всем имеющимся на этом компьютере файлам, а также файлам, которые открыты для просмотра на этом компьютере.

Частичным решением в такой ситуации может служить назначение привилегированного доступа к файлам для сотрудников различных отделов и уровней доступа.

3. Следует быть внимательным с флэш-картами

В настоящий момент очень многие люди не думают о том, чтобы, вставляя USB– флэш карту в компьютер ее сканировать. Более того, часто бывают случаи, во время которых люди могут просто найти такой съемный диск и подключить его к своему компьютеру. Это может быть очень опасным действием.

Опыт показывает, что около 60% людей, найдя в офисе флэш-карту, вставляют ее в свой компьютер. Если на такой флэш-карте указан логотип фирмы, то вероятность того, что человек подключит ее к своему рабочему компьютеру увеличивается до 90%.

4. Фишинг

Очень многие работники с доступом в интернет нажимают на контекстную рекламу на сайтах компьютеров, где не установлен блокировщик рекламы и тем самым скачивают какое-либо вредоносное ПО на рабочий компьютер.

Для решения этой проблемы можно либо установить работникам на компьютеры блокировщик рекламы, либо ограничить им доступ в интернет.

5. Открытый доступ к личным средствам связи и техническим устройствам

Люди часто не задумываются о том, чтобы ставить пароль на собственные средства связи, такие как смартфоны, хотя оттуда у них имеется доступ к рабочей почте и различным аккаунтам. Доступ к таким устройствам получить очень легко, а через них можно добраться и к рабочим данным.

6. Не стоит использовать не проверенные точки wi-fi

Современная статистика показывает, что люди, которые путешествуют и подключаются к сети wi-fiиз отелей в последующем могут прослушиваться различными службами, собирающими информацию, вплоть до FBI.

7. Не стоит сидеть в социальных сетях с рабочего аккаунта

Очень многие молодые люди любят использовать различного рода социальные сети, но никто не задумывается над тем, что это может принести за собой некоторые вредные последствия, такие как скачивание вместе с какими-то данными вредоносного ПО на свой компьютер, предоставление доступа к камере или микрофону на ноутбуке компании и другие.

Таким образом, чтобы повысить безопасность данных вашей компании, требуется начать думать как хакер и увидеть наиболее уязвимые места. Как известно, самой уязвимой части любой автоматизированной системы является человек. То есть, для того, чтобы повысить безопасность компании в целом, следует обеспечить повышение технической грамотности персонала, чтобы каждый из его членов понимал насколько важно серьезно относиться к информации, доступ к которой они имеют.

Литература

1. Бьянка Швинска - Научно-популярное издание Perspektywypress // «RUSH S.A.» , - 2019. – № 10. – с. 22-23.;
2. Электронный ресурс – официальный сайт организации по кибербезопасности «PaloaltoNetworks» – адрес доступа :https://www.paloaltonetworks.com/ ;
3. Электронный ресурс – видео с международной конференции по информационной безопасности RSAConference, выложенное наYouTube под названием «ThinkandActLike a HackertoProtectYourCompany’sAssets»– адрес доступа :https://www.youtube.com/ .